IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MARGUERITE KUROWSKI and BRENDA MCCLENDON, on behalf of herself and others similarly situated,	)	
Plaintiffs,	)	
vs.	)	**Case No. 22 C 5380**
RUSH SYSTEM FOR HEALTH d/b/a RUSH UNIVERSITY SYSTEM FOR HEALTH,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

MATTHEW F. KENNELLY, District Judge:

Marguerite Kurowski and Brenda McClendon (collectively Kurowski) have filed a complaint against Rush University System for Health (Rush) on behalf of a putative class of similarly situated persons. Kurowski alleges that Rush non-consensually and deceptively embedded third-party source code on its website and its MyChart patient portal. She further alleges that this source code, which is not visible to users of the website and portal, causes transmissions of her personally identifiable patient data to Facebook, Google, and Bidtellect for advertising purposes.

Kurowski filed this suit in federal court under the Class Action Fairness Act, 28 U.S.C. § 1332(d). She asserts claims for: (1) violations of the federal Wiretap Act as amended by the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2511(1)(a), (c)-(d) and 18 U.S.C. § 2511(3)(a); (2) breach of an implied duty of

confidentiality; (3) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA), 815 ILCS 505/2; (4) violations of the Illinois Uniform Deceptive Trade Practices Act (DTPA), 815 ILCS §§ 510/2(a); and (5) intrusion upon seclusion. Rush has moved to dismiss under Fed. R. Civ. P. 12(b)(6) for failure to state a claim upon which relief may be granted. For the reasons discussed below, the Court dismisses all of Kurowski's claims other than her DTPA claim.

Background

Rush is a non-profit health system headquartered in Chicago. Kurowski and McClendon are both Illinois residents. The complaint states that Kurowski has been a Rush patient since approximately 2017 and that McClendon has been a Rush patient since approximately 1999. Both allege that they have been MyChart patient portal users since 2017.

Rush maintains web properties for its patients to obtain information related to care at Rush and—at least with respect to MyChart—exchange communications about appointments, billing, test results, prescription refills, and other treatment. For example, the homepage of Rush's website offers tools to patients such as "Find a Doctor," or "Schedule Appointment." Rush's website is publicly available. Rush's MyChart patient portal, however, is available only to Rush patients. On MyChart, patients can, among other functions, access their test results or directly message their provider. The MyChart portal "is a software system designed and licensed to Rush by Epic Software Systems," a privately owned, third-party software company. Compl. ¶ 25.

Kurowski alleges that she has a reasonable expectation of privacy "in [her] personally identifiable data and communications exchanged with Rush" that derives

from her status as a patient, Rush's common law obligation to maintain patient confidentiality, state and federal laws and regulations, and Rush's express and implied promises of confidentiality. *Id*. ¶ 20. Kurowski alleges that the latter category, the express and implied promises of confidentiality, came via Rush's "Web Privacy Statement." The statement, which is linked at the bottom of Rush web properties, declares that "[Rush] do[es] not share information collected through the website with any third-party advertisers." Mot. to Dismiss, Ex. B. It also states:

> This website uses cookies to track how visitors use the website . . . . Users should be able to change browser settings to disable cookies . . . . Like many websites, www.rush.edu uses Google Analytics to gather information about how visitors use the website. Users may opt out if they do not want their data to be used by Google Analytics. Visit Google to learn how.

Id.

Kurowski alleges that her reasonable expectation of privacy was violated by Rush's allegedly secret deployment of "custom analytics scripts"—for example, Google Analytics—within its web pages and within MyChart. *Id*. ¶ 29. Kurowski alleges that Rush deployed this source code without her knowledge, consent, or authorization. This source code, she alleges, allows for the "contemporaneous unauthorized interception and transmission of personally identifiable patient data and redirection of the precise content of patient communications with Rush" whenever a Rush patient uses a Rush web property. *Id.* ¶¶ 5, 30. The data Kurowski alleges was transmitted to Facebook, Google, and Bidtellect includes patient IP addresses,[1] patient cookie identifiers,[2] device

[1] An IP address is a number that identifies a computer connected to the Internet.
[2] A cookie is a small text file that a web server can place on a person's web browser whenever the browser interacts with the website server. Cookies are often used and

identifiers, account numbers, URLs, other "unique identifying numbers, characteristics, or codes," and browser-fingerprints. *Id.* ¶ 33.

According to the complaint, the following is a shorthand description of how Kurowski alleges such patient data is transmitted in the background of Rush patients' day-to-day use of Rush web-properties.[3] Web browsers use two basic commands to communicate with website servers: a GET request (typically used to retrieve data via a search or a click) and a POST request (typically used to send data that is entered onto a website and then submitted). Third parties often acquire the content of user communications through something called a web bug, which is either camouflaged directly on the page or funneled through an invisible tag manager. Kurowski alleges that "Rush deploys Google Tag Manager on its websites through an 'iframe,' a nested 'frame' that exists within the Rush web property that is, in reality, an invisible window through which Rush funnels web bugs for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients." *Id*. ¶ 53.

Thus, when a patient clicks on a button that says "Schedule Your Appointment Now," Rush "causes the transmission of the patient's personally identifiable data and re-directs the content of the patient's click of the 'Schedule Your Appointment Now' button to [third parties such as] Facebook." *Id.* ¶ 61. The complaint includes screenshots of

---

sold by data companies to identify and track Internet users to sell advertising that is customized in light of a person's communications and habits.

[3] Kurowski alleges that she used a commercially available software application called Fiddler to test how Rush's various applications and source codes operate. This, the complaint states, allowed her to capture and record communications and other data transmissions flowing to and from www.rush.edu.

the kinds of data that would hypothetically be disclosed to third parties during this interaction, namely, that "the patient engaged in an event ('ev') labeled 'SubscribedButtonClick,' that the 'buttonText' was 'Schedule Your Appointment Now,' that the button was clicked from https://www.rush.edu, and the details of the first-party fbp cookie assigned by Rush." *Id.* ¶ 62. Rush refers to this data as purely metadata that is commonly transmitted during routine Internet usage. Kurowski disputes that characterization and alleges that the data does include identifying information (such as a patient's IP address, cookie identifiers, and—if the first two are blocked—browser fingerprints) that can be used to direct targeted advertising to patients.

Kurowski alleges that the value of data extracted "from people who use the Internet is well understood and generally accepted in the e-commerce industry." *Id.* ¶ 134. She therefore alleges that Rush profited from the patient data it disclosed to Facebook, Google, and Bidtellect without obtaining the patients' authorization.

Discussion

To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), the complaint must state a claim to relief that is plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The court must view the complaint "in the light most favorable to the plaintiff, taking as true all well-pleaded factual allegations and making all possible inferences from the allegations in the plaintiff's favor." *AnchorBank, FSB v. Hofer*, 649 F.3d 610, 614 (7th Cir. 2011). Even so, the plaintiff must provide "some specific facts to support the legal claims asserted" and cannot rely on conclusory allegations to make his claim. *McCauley v. City of Chicago*, 671 F.3d 611, 616 (7th Cir. 2011).

A. Wiretap Act claims

In count one, Kurowski alleges violations of the ECPA. The ECPA (also known as the Wiretap Act) provides that "any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication" may be subject to (among other things) a civil penalty. 18 U.S.C. § 2511(1)(a), (5)(a)(ii). The same is true for any person who intentionally discloses or uses, or endeavors to disclose or use, the contents of an intercepted communication. 18 U.S.C. § 2511(1)(c), (d). Section 2511(2)(d) of the statute provides an exception when the person intercepting a communication "is a party to the communication or where one of the parties to the communication has given prior consent to such interception." This so-called "party exception" does not apply, however, if the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d). In addition, section 2511(3)(a) provides that "a person or entity *providing an electronic communication service to the public* shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication . . . ." 18 U.S.C. § 2511(3)(a) (emphasis added).

1. Party exception

Rush contends that, as a party to the communications between it and its patients that Facebook, Google, and/or Bidtellect allegedly intercepted, it cannot be held liable for interception under the Wiretap Act. Kurowski disagrees, contending that Rush's

secret duplication and forwarding of unknowing patients' data to Facebook, Google, and/or Bidtellect precludes Rush from invoking the party exception. Kurowski further contends that, even if Rush could theoretically invoke the party exception, it is precluded from doing so because its conduct falls within the "criminal or tortious exception" to the party exception found in section 2511(2)(d).

Few circuits have addressed this exact issue, and those that have are split on how it should be decided. The Third Circuit has held that, when the defendant is the intended recipient of a communication, it is necessarily "one of its parties" and its interception of the communication is therefore shielded by the party exception. *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 142-43 (3d Cir. 2015) ("Because the defendants were the intended recipients of the transmissions at issue—i.e. GET requests that the plaintiffs' browsers sent directly to the defendants' servers—we agree that § 2511(2)(d) means the defendants have done nothing unlawful *143 under the Wiretap Act."); *see also*, *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 275–76 (3d Cir. 2016) (citing *In re Google Cookie* for the same proposition).

The Ninth Circuit, however, has held that an entity's simultaneous, unknown duplication and forwarding of GET requests made to a web page's server does not qualify for the party exemption, because holding otherwise "would render permissible the most common methods of intrusion, allowing the exception to swallow the rule." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020). The court placed emphasis on the Wiretap Act's legislative history and Congress's intent to "prevent the acquisition of the contents of a message by an unauthorized third-party or an unseen auditor." *Id.* (internal quotation marks omitted). It also considered

persuasive two cases decided by the First and Seventh's Circuits. *Id.* ("We adopt the First and Seventh Circuits' understanding that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception.").

But the "understanding" reached by the First and Seventh Circuits, and then relied on by the Ninth, involved whether an interception occurred at all, not whether the defendants could be considered a party to the intercepted communication. For example, the First Circuit held that a defendant could face liability under the Wiretap Act for intercepting a communication between a user and a third-party website via software that automatically duplicates the communication and sends it to the defendant. *See In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 22 (1st Cir. 2003). In that case, the First Circuit grappled with the defendant's argument that no interception occurred because there were two separate communications: the one between the user and the third-party and the one between the user and the defendant. The court rejected that argument, finding that an interception had occurred because the communication and the interception were contemporaneous.

Similarly, the Seventh Circuit held, in the case cited by the Ninth Circuit, that a defendant violated the Wiretap Act when he employed software that instructed his employer's email to duplicate and forward all e-mails the employer received to the defendant's own inbox. *United States v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010) (holding that because the copies were sent contemporaneously with the original e-mails, the defendant had intercepted the communications and could be held liable).

Thus, to the extent that the Ninth Circuit relied on *In re Pharmatrak* and

Szymuszkiewicz to reach its conclusion on the party exception—and it appears that it did—that reliance is not persuasive. The question here does not turn on the contemporaneousness of the alleged interception but rather, as the Third Circuit determined, who the intended recipient of the communication was. The Court concludes that Rush—and not Facebook, Google, or Bidtellect—was the intended recipient of the allegedly intercepted communications here. Rush is therefore a party to those communications and cannot be liable under the Wiretap Act for its alleged interception of them, if such an interception even occurred.

The "exception" to the party exception for criminal or tortious intent does not apply. Kurowski contends that Rush could be prosecuted under a provision of the Health Insurance Portability and Accountability Act (HIPAA), 43 U.S.C. § 1320(d)(6), for knowingly "disclosing individually identifiable health information" to third parties.[4] That statute defines "individually identifiable health information" as:

> any information, including demographic information collected from an individual, that— (A) is created or received by a health care provider . . . and (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual*, and— (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

43 U.S.C. § 1320(d)(6) (emphasis added). Kurowski has not alleged sufficient facts, however, to support an inference that Rush disclosed its patients' individually identifiable health information, at least as that term is defined by the statute.

[4] Kurowski adds "for commercial reasons" at the end of her recitation of what the statute prohibits. But section 1320(d)(6) mentions "for commercial advantage" only as a basis for a heightened fine and/or sentencing range, not for culpability.

Kurowski relies heavily on recent guidance issued by the Department of Health and Human Services (HHS) that suggests online tracking technologies may violate HIPAA. Rush correctly points out, however, that such regulatory guidance only applies prospectively. *Chrysler Corp. v. Brown*, 441 U.S. 281, 302 n. 31 (1979). Though it is plausible that the data transmitted via third-party source code constitutes more than just "metadata," as Rush contends, Kurowski fails to allege how the hypothetical data disclosures described in the complaint involve "the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual." 43 U.S.C. § 1320(d)(6); *see also*, *Smith v. Facebook, Inc*., 745 F. App'x 8, 9 (9th Cir. 2018) ("Information available on publicly accessible websites stands in stark contrast to the personally identifiable patient records and medical histories protected by these statutes—information that unequivocally provides a window into an individual's personal medical history."). Moreover, the hypotheticals provided by Kurowski appear to illustrate only what occurs when an individual—whether a patient or not—clicks on certain areas of Rush's public website. Kurowski does not allege what surreptitious patient data disclosures occur when an actual Rush patient enters her MyChart portal and navigates through it.

For these reasons, Rush cannot be held liable for interception of the alleged communications, and the Wiretap Act's criminal or tortious conduct exception to the statute's party exception does not apply.

2. Electronic communication service

The second type of claim under the Wiretap Act that Kurowski includes in count 1

is the alleged violation of section 2511(3)(a). Section 2511(3)(a) prohibits the provider of an "electronic communication service" from divulging the content of communications transmitted on that service to third parties (i.e., anyone other than the addressee or the intended recipient). Rush contends that it is not an electronic communication service provider and that Kurowski has not sufficiently alleged the contents of her communications with Rush. Kurowski contends that, by providing access to the MyChart patient portal—which allows patients to communicate directly with their providers—Rush acts as an electronic communication service. Kurowski also contends that she has alleged sufficient facts to support an inference that, as a patient who was encouraged to sign up for an utilize MyChart, she communicated with her provider on that platform and those communications were disclosed via third-party source code embedded within it. The Court agrees with Kurowski's latter contention,[5] but not the former.

An "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Kurowski appears to allege that Rush's licensing of MyChart, and its offering of that platform as a resource to its patients, makes Rush an electronic communication service. It is, of course, true that the MyChart portal allows patient users to send and receive communications to and from their providers. But Rush cannot plausibly be considered an electronic communications service provider within the meaning of the

[5] Although Kurowski fails to identify specific protected information or data allegedly disclosed to third parties, one may reasonably infer from her allegations that transmission of her data via third-party tracking source code is at least plausible. Kurowski's entitlement to this inference is not, however, dispositive of this issue for reasons explained below.

Act. Rush is simply a licensee; it licenses from Epic, a non-party, the service that facilitates the electronic communication. Rush cites several cases on page eight of its motion to dismiss that Court finds persuasive on this point. These cases uniformly hold that companies that merely purchase or use electronic communications services in the conduct of their ordinary business are not themselves electronic communications services. *See Garner v. Amazon.com*, *Inc*., 603 F. Supp. 3d 985, 1003–04 (W.D. Wash. 2022) ("A company that merely utilizes electronic communications in the conduct of its own business [here, Amazon's "Alexa"] is generally considered a purchaser or user of the communications platform, not the provider of the service to the public."); *In re Jetblue Airways Corp. Priv. Litig.*, 379 F. Supp.2d 299, 307 (E.D.N.Y. 2005) (Jetblue's passenger reservations system is not an electronic communications service). And in the case Kurowski relies on, *Pascal Pour Elle, Ltd. v. Jin*, 75 F. Supp. 3d 782 (N.D. Ill. 2014), Judge Durkin found that a software program that provides salons the ability to communicate with its customers by e-mail—not the salon offering the program itself—to be an electronic communication service. Unlike Epic—the licensor of the MyChart platform on which patients can communicate with their provider—hospital systems such as Rush are not in the electronic communications business.

The Court therefore dismisses count one.

B. Breach of the implied duty of confidentiality

In count two of her complaint, Kurowski asserts a common law claim for the breach of an implied duty of confidentiality. She bases this claim on the theory that every patient-health care provider relationship implies a contract and that a provider's disclosure of a patient's private health information constitutes a breach of that contract.

Rush contends that Illinois law does not recognize a cause of action in tort for this conduct, and it contends that even if such a cause of action exists, its scope is limited to disclosures that violate the statutory physician-patient privilege.[6] The Court agrees with Rush.

Kurowski relies predominantly on *Geisberger v. Willuhn*, 72 Ill. App. 3d 435, 390 N.E.2d 945 (1979), in which the court held that "the breach of a confidential relationship and the breach of contract are probably co-extensive." *Id.* at 438, 390 N.E.2d at 948. It therefore held that, because the disclosure of a patient's name alone—rather than "the publication of facts relating to either the [patient's] medical condition or the physician's diagnosis or treatment"—did not violate the statutory privilege, such a disclosure did not constitute an invasion of privacy. *Id.* at 439, 390 N.E.2d at 948. Thus, only the disclosure of "information relating to the patient's mental or physical condition or the physician's diagnosis or treatment"—which is the type of disclosure that would violate the statutory physician-patient privilege—would be actionable under Kurowski's theory. *Id.* at 438, 390 N.E.2d at 948.

Kurowski fails to allege the disclosure of any information related to the provision of treatment to her or other similarly situated Rush patients. One of the hypothetical disclosures described in the complaint merely discloses that "the patient engaged in an event ('ev') labeled 'SubscribedButtonClick,' that the 'buttonText' was 'Schedule Your Appointment Now,' that the button was clicked from https://www.rush.edu, and the details of the first-party fbp cookie assigned by Rush." Compl. ¶ 62. The Court notes

[6] "No physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character, necessary to enable him or her professionally to serve the patient." 735 ILCS § 5/8-802.

first that this hypothetical illustrates what occurs when a user interacts with Rush's public webpage, not the MyChart portal. The "GET" and "POST" requests described in the complaint "can be made by any visitor to Rush's website, whether patient or not." Def.'s Mot. to Dismiss at 11. But even if one could reasonably infer that this information identifies an individual patient by name, this sort of disclosure does not violate physician-patient statutory privilege. *See Geisberger*, 72 Ill. App. 3d at 438, 390 N.E.2d at 947 ("We follow the overwhelming majority of the courts of the United States which have held that the disclosure of the name alone of the patient by a doctor or his agents does not violate the patient-doctor privilege established by [Ill. Rev. Stat.1973, ch. 51, P 5.1].").

Kurowski attempts to work around this well-established requirement by contending that the recent HHS guidance confirms that "tracking on user-authenticated patient portals is prohibited by HIPAA." Pls.' Resp. to Mot. to Dismiss at 11. The Court has already noted, however, that the HHS guidance provided by Kurowski is not controlling and only applies prospectively.

Finally, Kurowski contends that Rush's HIPAA privacy notice additionally implies an expectation of privacy that was breached by Rush's alleged secret deployment of third-party source code. Def.'s Mot. to Dismiss, Ex. A. The notice states that "Each time you visit a hospital, physician or other health care provider, a record of your visit is made." *Id*. at 1. The notice further states that "[t]his record typically contains information *regarding your symptoms, diagnosis, examination and test results, current and future treatment . . . ." Id.* (emphasis added). The notice applies to "all records *regarding your care* generated by Rush University Medical Center or Rush Oak Park

Hospital, Inc. . . . whether made or received by our organization's personnel or given to others outside the organization for business purposes." *Id.* (emphasis added). Thus like the statutory physician-patient privilege, Rush's privacy notice contemplates the protection of care-related patient information. It does not contemplate the protection of a patient's name, IP address, cookie identifier, or other device-related identifying information unconnected with information about the patient's care.

The parties advance additional arguments regarding the availability of a common law cause of action for breach of confidentiality in Illinois. But because the Court has concluded that—if such a cause of action exists—it is co-extensive with the statutory patient-physician privilege that Kurowski has not alleged was violated, the Court need not address those arguments. The Court therefore dismisses count two.

C. ICFA claim

In count three of her complaint, Kurowski alleges that Rush engaged in "deceptive acts and practices," Compl. ¶¶ 229-30, and "unfair acts and practices," *id.* ¶¶ 223, 233, in violation of the ICFA. The former claim is based on the allegation that Rush made misrepresentations in its privacy statement; the latter is based on Rush's alleged disclosure of patient data without obtaining their authorization. "In order to state a claim under the ICFA, a plaintiff must show: (1) a deceptive or unfair act or promise by the defendant; (2) the defendant's intent that the plaintiff rely on the deceptive or unfair practice; and (3) that the unfair or deceptive practice occurred during a course of conduct involving trade or commerce." *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739 (7th Cir. 2014) (internal quotation marks omitted).

Regarding the "deceptive acts and practices" aspect of Kurowski's ICFA claims,

the parties make several contentions regarding the sufficiency of Kurowski's allegations on whether, and how, she was *personally* deceived by Rush's privacy statement. But both the "deceptive acts and practices" and "unfair acts and practices" claims fail for a more basic reason: Kurowski has failed to allege actual, pecuniary loss as required by the ICFA.

An individual suing under the ICFA must "plead that the deceptive or unfair act caused her to suffer actual damages, meaning pecuniary loss." *Benson v. Fannie May Confections Brands, Inc.*, 944 F.3d 639, 647 (7th Cir. 2019). "In the . . . case of a private ICFA action brought by an individual consumer, actual loss may occur if the seller's deception deprives the plaintiff of 'the benefit of her bargain' by causing her to pay 'more than the actual value of the property.'" *Kim v. Carter's Inc.*, 598 F.3d 362, 365 (7th Cir. 2010) (quoting *Mulligan v. QVC, Inc.*, 382 Ill. App. 3d 620, 627-28, 888 N.E.2d 1190, 1197-98 (2008)). Kurowski invokes the "benefit of the bargain" theory of damages; she alleges that she and other patients suffered monetary loss by "overpaying for Rush's health care services." Compl. ¶ 238. Kurowski further alleges that she suffered non-monetary injuries to her privacy.

There is no basis under Illinois law to suggest that Kurowski is entitled to claim a "privacy injury" under ICFA. *See Khorloo v. John C. Heath Attorney at Law*, No. 18 C 1778, 2020 WL 1530735, at *2 (N.D. Ill. Mar. 31, 2020) ("[T]he Court could not locate any Illinois case law suggesting that privacy violations . . . provide a basis for actual damages under the ICFA. It seems unlikely that the statute allows plaintiffs to recover damages for privacy violations because the ICFA is concerned with fraudulent or unfair advertising, not with individual privacy rights."). Kurowski's "benefit of the bargain"

theory of damages also lacks merit. There is no charge for use of Rush's web properties, and Kurowski's ICFA claims are not breach of contract claims. And nowhere in the complaint does Kurowski allege (nor would it appear that she could allege plausibly) that she or other patients received a lower quality of health care because of Rush's use of third-party source code on its web properties.

For these reasons, the Court dismisses count three.

D. DTPA claims

In count four of Kurowski's complaint, she alleges that Rush engaged in deceptive trade practices that violate the DTPA. More specifically, Kurowski alleges that Rush represented that "good or services have characteristics that they do not have"—or were "of a particular standard, quality, or grade," when in fact they were "of another." Compl. ¶ 243. She further alleges that Rush's practice of disclosing patients' data without their knowledge or consent also violates the DTPA. Kurowski seeks both monetary and injunctive relief for her alleged injuries under the statute.

"The IDTPA does not support a claim of actual or punitive damages, however, as the 'only remedy under the [IDTPA] is injunctive relief.'" *Kljajich v. Whirlpool Corp., No.*, No. 15 C -5980, 2015 WL 12838163, at *5 (N.D. Ill. Sept. 25, 2015) (quoting *Vara v. Polatsek*, No. 1–11–2504, 2012 WL 6962887, at *13 (Ill. App. Ct. Oct. 5, 2012)). Kurowski alleges that her claim for damages under DTPA survives because it is brought alongside her ICFA claim for the same conduct. *See Duncavage v. Allen*, 147 Ill. App. 3d 88, 102, 497 N.E.2d 433, 441 (1986) (a plaintiff may use an alleged violation of the DTPA to recover damages under ICFA). But, as just addressed, the Court has dismissed Kurowski's ICFA claim for her failure to allege pecuniary damages. Kurowski

cannot bootstrap an otherwise impermissible claim for damages under the DTPA via her deficient claim under ICFA.

Thus, all that remains is Kurowski's claim for injunctive relief under the DTPA. "In order to maintain [an action for injunctive relief under the DTPA], the consumer must allege facts which would indicate that he is likely to be damaged in the future." *Popp v. Cash Station, Inc.*, 244 Ill. App. 3d 87, 99, 613 N.E.2d 1150, 1157 (1992) (internal quotation marks omitted). Rush contends that Kurowski has not sufficiently alleged future harm because, to the extent that Rush *is* deceiving patients (which it disputes), Kurowski's awareness of this deception "arms her with the knowledge she needs to avoid any future harm . . . ." Def.'s Mot. to Dismiss at 17 (quoting *Kljajich*, 2015 WL 12838163, at *4).

The Court disagrees. Kurowski remains a patient of Rush and thus must engage with Rush web properties to continue receiving medical care. Rush has not suggested that it has stopped its use of the alleged third-party source code that Kurowski alleges causes disclosure of her and other patients' private data. Thus, the future harm that Kurowski and other similarly situated Rush patients face by continuing to use Rush web properties is sufficient at the present stage to support her claim for injunctive relief under the DTPA.

E. Invasion of privacy claim

In count five of the complaint, Kurowski alleges that Rush invaded her and other patients' privacy by intrusion upon seclusion. Kurowski alleges that Rush intruded by deploying third-party source code that caused personally identifiable patient data to be disclosed to third parties. Rush contends that Kurowski does not state a claim for

intrusion upon seclusion because she fails to satisfy the first element of the claim: an unauthorized intrusion. Kurowski contends that she has satisfied that requirement because "both the initial collection and the subsequent dissemination are alleged to have been conducted without Plaintiffs' knowledge or consent." Pls.' Resp. to Mot. to Dismiss at 17. The Court agrees with Rush.

In *Dinerstein v. Google, LLC*, 484 F. Supp. 3d 561 (N.D. Ill. 2020), Chief Judge Pallmeyer concluded that "[t]he Illinois Supreme Court has explained that 'the core of this tort is the offensive prying into the private domain of another' and that '[t]he basis of the tort is not publication of publicity.'" *Id.* at 594 (quoting *Lovgren v. Citizens First Nat. Bank of Princeton*, 126 Ill. 2d 411, 417, 534 N.E.2d 987, 989 (1989)). Thus, "disclosures of private personal information 'do not support a claim for unauthorized intrusion.'" *Id*. (citing *In re Trans Union Corp. Privacy Litig*., 326 F. Supp. 2d 893, 902 (N.D. Ill. 2004)).

The Court adopts the same view here. The question is therefore whether Kurowski has alleged sufficient facts to allow an inference that Rush intruded upon its patients' seclusion when it allowed third-party source code to collect the data Kurowski alleges it later disclosed. The Court concludes she has not.

It is clear from Kurowski's complaint that the core of her claim is Rush's deployment of third-party source code that causes the transmission of patient data. As discussed with respect to count 1, the allegedly intercepted communications were intended to reach Rush. This is underscored by the theme underlying most of Kurowski's allegations, namely, that patients trusted that communications and queries directed at Rush, their health care provider, would be kept private. In other words, the

harm for which Rush is responsible, if any, is its disclosure of patient data (which, as alleged, is not protected private health information)—not the obtaining of that data. The actual intrusion upon patients' seclusion, via interception of their communications, is carried out by third parties. As Rush correctly points out, the cases relied on by Kurowski involved intrusions made by third parties, "not voluntary communications with defendant that were allegedly disclosed." Def.'s Reply at 14.

Because Kurowski has failed to allege sufficient facts to support a claim for intrusion upon seclusion upon which relief can be granted, the Court dismisses count 5.

Conclusion

For the reasons stated above, the Court grants defendant's motion to dismiss [20] as to counts one, two, three, and five of the complaint but denies the motion as to count four. Defendant is directed to answer count four by no later than March 24, 2023. A telephonic status hearing is set for April 10, 2023 at 9:05 a.m., using call-in number 888-684-8852, access code 746-1053. A joint status report concerning the status of discovery and any settlement discussions is to be filed on April 3, 2023.

Date: March 2, 2023

MATTHEW F. KENNELLY
United States District Judge